Literatur

Ellen Schlüchter, Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität. Kommentar mit einer kriminologischen Einführung (Motive-Texte-Materialien, Bd.42). *Heidelberg: C.F.Müller Juristischer Verlag.* XXV, 207 S. *1987.*

Das *Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität* (1986) hat dem Strafgesetzbuch, dem Gesetz gegen den unlauteren Wettbewerb und dem Börsengesetz eine Sequenz von Straftatbeständen inkorporiert, deren Kern das sog. *Computerstrafrecht* bildet. Es umfaßt — von bestimmten Sonderformen der Vermögenskriminalität abgesehen — den Geheimnisschutz von Daten (§ 202a StGB) sowie ihren Schutz vor Veränderung (§ 303a, 303b StGB) und Fälschung (§ 269, 270 StGB). Mit der Konzipierung dieser Delikte enthält das deutsche Recht einen systematisch angelegten, umfassenden strafrechtlichen Schutz gegen bestimmte EDV-Manipulationen. Verf. reiht sich mit ihrem Kommentar mutig in die juristische Avantgarde ein, wenn sie der in diesen Fragen besonders hilfsbedürftigen Rechtspraxis mit ihren Erläuterungen zur Hand gehen möchte.

Für die suggestive Zusammenfassung der genannten Delikte im Begriff der Wirtschaftskriminalität ist nicht *Verf.,* sondern der Gesetzgeber verantwortlich. Tatsächlich ist eine solche Akzentuierung wenig erhellend, kriminalpolitisch allenfalls irreführend. Automatische Datenverarbeitung ist keine Domäne von Wirtschaft oder Verwaltung, sondern ein *universell* anwendbares Mittel zur Aufnahme und Verknüpfung von Daten. Wenn daher besondere Schutzbedürfnisse bestimmter Anwender zum Maß der Gesetzgebung genommen werden, so entsteht die Gefahr einer strafrechtlichen Überreaktion, die den kriminalpolitischen Sinn des Gesetzes diskreditieren und die Praxis vor schwer zu lösende Probleme stellen würde. Was für sensible Dateien von Forschungseinrichtungen, Großbetrieben oder staatlichen Sicherheitsbehörden angemessen sein mag, mißrät in seiner Anwendung beispielsweise auf die Verhältnisse privater EDV-Amateure unfehlbar zu einer hypertrophen Kriminalisierung belangloser, alltäglicher oder sozialadäquater Verhaltensweisen.

Verf. läßt ihr Buch dem Gesetz in einem zeitlichen Abstand folgen, den man bislang von Referentenkommentaren gewohnt war. Um so mehr hätte man erwartet, daß die vorgeblichen kriminalpolitischen Notwendigkeiten analysiert worden wären, mit denen die neuesten Kreationen eines auf Modernität bedachten Gesetzgebers begründet worden sind. *Verf.* sieht ihre Aufgabe indessen vorwiegend in der Interpretation der gegebenen Normen, in die sie die verlautbarten Motive des Gesetzes wohlwollend einfließen läßt. Eine solche Beschränkung der literarischen Absichten bedarf keiner Rechtfertigung, läßt jedoch auch für das geltende Recht Fragen offen, die sich einer kriminalpolitischen Analyse erschlossen hätten. Präzision und Anschaulichkeit der Kommentierung hätten im übrigen gewonnen, wenn die technischen Grundlagen der Materie stärker in die Überlegungen einbezogen worden wären.

1. Den Tatbestand des *Ausspähens von Daten* (§ 202a StGB) interpretiert Verf. als einen Fall des *formalisierten* Geheimnisschutzes, also als strafrechtlichen Datenschutz ohne Rücksicht auf die inhaltliche Geheimhaltungswürdigkeit der Daten; das Delikt wird damit auch strukturell in unmittelbare Nachbarschaft zur Verletzung des Briefgeheimnisses (§ 202 StGB) gerückt. Diese Deutung berücksichtigt indessen nicht hinreichend, daß die besondere Art der Speicherung oder Übermittlung „nicht unmittelbar wahrnehmbarer" Daten (§ 202a Abs.2 StGB) keineswegs als Indiz für einen vermutbaren Geheimhaltungswillen oder gar für eine besondere inhaltliche Schutzwürdigkeit des Dateninhalts verstanden werden kann; denn die fehlende unmittelbare Wahrnehmbarkeit der Daten ist durch die technische Konzeption ihrer Verarbeitung, nicht aber durch die Absicht ihrer Maskierung bedingt. Das Gesetz verlangt deswegen auch kumulativ, daß die Daten „gegen unberechtigten Zugang besonders gesichert" sein müssen. Die Art dieser Sicherung ist nun aber gesetzlich weder formalisiert noch auch nur typisiert, so daß beliebige externe Sicherungen der Daten (Bewachung oder Verschluß der EDV-Zentrale etc.) für die Erfüllung des Tatbestandes ebenso genügen wie logische (interne) Sperren, mit denen die Daten selbst versehen sind (Paßwort etc.). Solche Sperren dienen aber vielfach vorrangig der Betriebssicherheit der Anlage und lassen sich daher nur bedingt als Ausdruck eines Geheimhaltungswillens verstehen. Die Schutzstruktur des § 202a StGB weist daher eher Ähnlichkeiten mit der des Hausfriedensbruchs auf, ohne dessen Typisierungsgrad zu erreichen oder seiner Funktionalität zu entsprechen. Die Formalisierungsthese bedarf daher in mehrfacher Hinsicht der Modifizierung.

Ernstliche Auslegungsprobleme ergeben sich daraus, daß die Tathandlung nach dem Gesetzeswortlaut nicht auf die Überwindung der geforderten Zugangssicherung bezogen zu sein braucht. Entfällt daher beispielsweise die Zugangsberechtigung mit dem Ablauf des Vertrages über die Nutzung einer Datenbank, so ist eine unbefugte Fortsetzung der Abfragen unter Weiterverwendung des zugeteilten Paßwortes strafbar, obwohl es dem Betreiber ersichtlich nicht um Geheimhaltung, sondern um die Lizenzgebühren geht. Für den

farblosen Begriff des „Verschaffens" von Daten genügt im übrigen neben jeder anderen Form der Bemächtigung die Kenntnisnahme vom Dateninhalt. Es ist daher unrichtig, wenn *Verf.* das sog. *Hacking,* also das Eindringen in fremde Rechnersysteme, mit der Gesetzesbegründung und der ihr folgenden Literatur als straflos bezeichnet; denn nach Überwindung der (logischen) Zugangssperren nimmt der Eindringling selbstverständlich und unvermeidlich einen Teil derjenigen Daten und Programme wahr, mit denen das betreffende System arbeitet, mögen die erworbenen Informationen nun geheimhaltungswürdig sein oder nicht. Kaum haltbar dürfte auch die weitere, für die Praxis ungleich wichtigere Annahme der *Verfasserin* sein, daß das unbefugte *Kopieren* geschützter Programme als Ausspähen von Daten nach § 202a StGB strafbar sei. Denn durch das Kopieren des Programms wird nichts „verschafft", was in der Form des Originals bei dem Täter nicht ohnehin schon vorhanden gewesen wäre; und vor allem ist der Kopierschutz kein Schutz gegen den unberechtigten „Zugang" zum Programm, das trotz des Kopierschutzes für die Benutzung gerade zur Verfügung steht.

Über den kriminalpolitischen Sinn der zuvor begründeten Annahmen wird man mit guten Gründen streiten können; daß solche Meinungsverschiedenheiten indessen im Hinblick auf die Interpretation eines soeben verabschiedeten Gesetzes auszutragen sind, dürfte jede Reformeuphorie nachhaltig dämpfen. Tatsächlich dürften die Überlegungen, die die *Verfasserin* zur Auslegung des Tatbestandes zusammengetragen hat, kaum mehr als einen Vorgeschmack auf die Komplikationen geben, vor die die Praxis alsbald gestellt sein wird.

2. Den der Sachbeschädigung analogen Tatbestand der *Datenveränderung* (§ 303a StGB) legitimiert *Verf.* mit dem hohen Wert der Daten und der zunehmenden Abhängigkeit der Wirtschaft von ihrer Integrität. Daß dies nur auf einen — vermutlich kleineren — Teil der Daten zutrifft, wurde schon einleitend bemerkt. Zudem sind die Zweifel an der kriminalpolitischen Notwendigkeit der neuen Strafnorm hiermit nicht behoben; denn jedenfalls gespeicherte Daten sind über das Eigentum an den Datenträgern in den Schutzbereich der Strafvorschrift gegen *Sachbeschädigung* (§ 303 StGB) einbezogen. Die hiergegen gelegentlich geäußerten Bedenken, die *Verf.* kommentarlos referiert, sind weder begründet noch können sie ernstlich zur Legitimation einer neuen Strafvorschrift dienen. Zur Auslegung der Gesetze ist die Rechtsprechung berufen; man hätte mit der Konstituierung einer neuen Strafvorschrift daher — wie im Falle des § 266b StGB — jedenfalls zuwarten sollen, bis sich praktische Unzuträglichkeiten ergeben hätten. Im übrigen stellt § 303a StGB nicht lediglich klarstellend die Beschädigung von fremden Datenträgern unter Strafe, sondern die Veränderung von Daten ohne Rücksicht auf ihr körperliches Substrat, so daß auch Daten im Stadium der Übermittlung erfaßt werden. Ob hierfür ein spezifisches kriminalpolitisches Bedürfnis besteht, ist empirisch keineswegs belegt und zweifelhaft, zumal schon die *Datennetze* als solche einen gewissen strafrechtlichen Schutz gegen störende Manipulationen bieten. Mit der Ersetzung des Eigentums durch den vagen Begriff des Datums als geschütztem Rechtsgut geht vor allem der sichere normative Anknüpfungspunkt der Fremdheit verloren, der für den Unrechtstypus der Sachbeschädigung konstitutiv ist. Die neue Strafnorm des § 303a StGB bedroht deswegen (u.a.) das Löschen von Daten *ohne jede weitere Präzisierung* mit Strafe. Da nun kein Rechner und kein Programm ohne das fortwährende Löschen und Verändern von Daten funktionsfähig ist, sind die inkriminierten Vorgänge als solche ebensowenig Unrecht wie das Anschalten des Rechners, durch den sie erzeugt werden. Offenbar baut das Gesetz darauf, daß der Rechtsanwendung gelingen werde, was die Gesetzgebung versäumt hat, nämlich die Konstituierung des *vollständigen* Unrechtstypus der Datenveränderung. Hierzu bedarf es der Prägung einer „Verfügungsberechtigung" über die fraglichen Daten und mithin einer rechtlichen Operation, deren Verläßlichkeit hinter der Prüfung der Eigentumsverhältnisse weit zurückbleibt. Dies zeigen die hierauf verwendeten Bemühungen der *Verfasserin* mit aller Deutlichkeit. Das „Löschen" von Daten ist technisch im übrigen nicht nur — wie *Verf.* anzunehmen scheint — durch deren Beseitigung (also durch Ummagnetisierung der Trägerschicht), sondern auch durch Entfernung der betreffenden Verzeichniseinträge (und der damit verbundenen Freigabe des reservierten Speicherplatzes für spätere Überschreibungen) gängig. Damit wird die Möglichkeit zur Restaurierung der fraglichen Datei (ebenso wie die Existenz simpler Sicherungskopien) zu einem Auslegungsproblem, das sich nicht einfach durch den Rückgriff auf ähnliche Fragestellungen im Bereich der auf körperliche Gegenstände zugeschnittenen Sachbeschädigung erledigen läßt, da das gespeicherte Datum als unkörperliche Information weiterbesteht. Hierzu äußert sich *Verf.* nicht.

3. Mit einiger Skepsis beurteilt *Verf.* schließlich den Tatbestand der *Datenfälschung* (§ 269 StGB), den sie vor Inpraktikabilität und Uferlosigkeit zugleich schützen möchte. Da der Urkundenbegriff des § 267 StGB visuelle Wahrnehmbarkeit der beweiserheblichen Gedankenerklärung voraussetzt, sind unlautere Manipulationen an nicht wahrnehmbaren Daten keine Urkundenfälschung. Der Tatbestand der Datenfälschung, der diese Lücke schließen soll, sucht sich nun der unbezweifelbaren kriminalistischen Dignität der Urkundenfälschung durch einen vorgeblichen Geniestreich zu versichern, Indem er die Strafbarkeit der Veränderung beweiserheblicher Daten davon abhängig macht, „da bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde". *Verf.* zeigt deutlich die Problematik einer solchen Fiktion, die sich ersichtlich darauf verläßt, daß die Merkmale des Urkundenbegriffs — von der visuellen Wahrnehmbarkeit der Gedankenerklärung abgesehen — bei gespeicherten Daten in einer der Urkundenfälschung entsprechenden Weise rekonstruiert werden können. *Verf.* setzt diese Hypothese völlig zu Recht in eine restriktive Interpretation des § 269 StGB um: die Manipulation von Daten ist nur